PDR RID Report

Date Last Modified 6/8/95
Originator Ernie Lucier
Phone No 202-358-0772
Organization NASA/YD
E Mail Address elucier@hq.nasa.gov
Document PDR FOS 1/17/95 Dean Moore
Section **Page** DM-3 **Figure Table**

RID ID PDR 134
Review CSMS
Originator Ref Presentation DM-3
Priority 1

Category Name Requirements **Actionee** Project
Sub Category RMA
Subject RMA Issues

Description of Problem or Suggestion:

IS MDT < 1 minute necessary? This drives the system architecture to a much higher availability than required.

Originator's Recommendation

Consider changing MDT to a larger number if a lower cost system will result.

GSFC Response by: Ellen Herring **GSFC Response Date** 5/17/95

The one minute or less mean down time (MDT) applies to FOS Critical Real-time functions which could result in a "Spacecraft emergency" if interrupted during their execution. This requirement is derived from the level 2 ECS requirement number 1392 which reads "The ECS shall have no single point of failure for functions associated with real- time operations" and 1249 which reads "Critical ECS functions shall have reliability, maintainability, and availability (RMA) requirements with availabilities and average down times commensurate with the level of criticality." These requirements trace to the level 3 requirement EOSD3800 which reads "The FOS shall have an operational availability of 0.9998 at a minimum (.99997 design goal) and an MDT of one (1) minute or less (0.5 minute design goal) for critical real-time functions that support: a. Launch b. Early orbit checkout c. Disposal d. Orbit adjustment e. Anomaly investigation f. Recovery from safe mode g. Routine real-time commanding and associated monitoring for spacecraft and instrument health and safety" and the level 3 requirement EOSD3810 which reads "The FOS shall have an operational availability of 0.99925 at a minimum (.99997 design goal) and an MDT of five (5) minutes or less (0.5 minute design goal) for non-critical real-time functions." EOC availability model summarizing system allocation is available upon request.

The implementation of these requirements implies at least two parallel strings. One in operation and the other in hot backup. This configuration will also satisfy the no single point failure requirement. These requirements also imply that the communications network between the EOC, EDOS, and White Sands needs to be redundant or fault isolated and switchable to the backup within one minute.

These requirements are reasonable and are in line with other programs at GSFC. It should be noted that as a by-product of the redundant architecture, availability numbers are considerably better than the specification requirements. However, because the down time of a single string will result in MDT of 4 hours which is totally unacceptable, the redundant architecture is the proper choice. In summary the requirements as allocated are appropriate. The design goals are ambitious and will be clocely monitored throughout the implementation process to insure that the design goals are not allowed to drive system architecture or development costs.

HAIS Response by: Forman **HAIS Schedule**
HAIS R. E. Armstrong **HAIS Response Date**

Status **Closed** **Date Closed** **6/8/95** **Sponsor** **Herring**

****** **Attachment if any** ******